

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with the Apple IDs:
hunchotez38@icloud.com and tarshartez@icloud.com,
stored at premises controlled by Apple Inc.

Case No.23-963M(NJ)

Matter No.: 2023R00230

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 8/3/2023 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

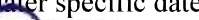
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/20/2023 @ 11:40 a.m.

, the later specific date of _____


Judge's signature

Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 60%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with hunchotez38@icloud.com and tarshartez@icloud.com (the “accounts”) that are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the accounts were created, the length of service, the IP address used to register the accounts, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- c. The contents of all emails associated with the accounts from January 1, 2023 to the present, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- d. The contents of all instant messages associated with the accounts from January 1, 2023 to the present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the

accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- f. All activity, connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- g. All records and information regarding locations where the accounts or devices associated with the accounts were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the accounts, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, those violations involving Tarsh A. SMITH and others known and unknown, and occurring after January 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The sale of illegal drugs and the laundering of proceeds of drug sales;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to drug trafficking, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with the Apple IDs:
hunchotez38@icloud.com and tarshartez@icloud.com,
stored at premises controlled by Apple Inc.

Case No.23-963M(NJ)

Matter No.: 2023R00230**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1)	Distribution of a controlled substance, conspiracy, and unlawful use of a
21 U.S.C. § 846	communication facility.
21 U.S.C. § 843(b)	

The application is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

MICHAEL
LOPEZ

Digitally signed by MICHAEL
LOPEZ
Date: 2023.07.19 12:49:20
-05'00'

Applicant's signature

TFO Michael Lopez, DEA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 7/20/2023

City and state: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Michael Lopez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. (“Apple”), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer with the Drug Enforcement Administration (DEA), and have been since March 2020. I am also a Police Officer with the Milwaukee Police Department and have been since September 2000.

3. As a part of my duties, I investigate criminal violations relating to narcotics trafficking offenses, including violations of Title 21, United States Code, Sections 841, 843, and 846, and federal firearms offenses, including violations of Title 18, United States Code, Sections 922(g), 924(a), and 924(c). In the course of my experience, I have and continue to be involved in investigations of criminal offenses and have assisted with search warrants for items related to gang investigations, organized crime, violent crime, firearms offenses, drug trafficking, thefts,

counterfeit crimes, forgeries, including cellular telephones and other electronic telecommunication devices.

4. I have had formal training in the investigation of drug trafficking. I have worked with numerous informants in the investigation of drug trafficking. I have participated in the execution of numerous search warrants in which controlled substances, firearms, drug paraphernalia, and counterfeit monies were seized.

5. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

6. This affidavit is based upon my personal knowledge and upon information provided to me by other federal, state, and local law enforcement officers during the course of their official duties. Throughout this affidavit, I refer to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom I have had regular contact regarding this investigation.

7. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Section 841(a)(1), 843(b), and 846 have been committed by Tarsh A. SMITH and others known and unknown. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

10. Case agents are currently investigating Tarsh A. SMITH (DOB: 03/27/90) who is selling cocaine, heroin, and fentanyl in the Eastern District of Wisconsin.

11. In June 2023, case agents initiated an investigation into SMITH who was identified by a confidential source as a person who was distributing large amounts of heroin in Milwaukee, Wisconsin.

12. During the preliminary investigation, case agents conducted a check that showed SMITH was on extended supervision with the Wisconsin Department of Corrections for Possess w/Intent-Cocaine (>5-15g), and 2nd-Degree Recklessly Endangering Safety under Milwaukee County case no. 15CF631.

13. Further investigation showed that on February 1, 2021, SMITH was charged with Possess w/Intent-Heroin (>10-50g) and Possess w/Intent-Cocaine (>1-5g) under Milwaukee County case no. 21CF380. According to Wisconsin’s Consolidated Court Automation Programs (CCAP), the date of the offenses was January 28, 2021. Case agents reviewed Milwaukee Police Department reports regarding the case and learned that the analysis of a cellphone linked to SMITH contained communications consistent with drug trafficking, including the sale of heroin.

14. Case agents searched CLEAR for any records for SMITH. CLEAR is a database containing public records available to law enforcement. Case agents have used this database in the

past and found it to be reliable and accurate. A search of CLEAR showed SMITH's last known address was 10430 West Innovation Drive, Apartment 112, Wauwatosa, WI.

15. On June 2, 2023, case agents served Community Manager Stacy Becker of Mandel Group, a property management company for 10430 West Innovation Drive, Wauwatosa, WI, an administrative subpoena for information related to Apartment 112. Becker confirmed SMITH is the lone tenant of 10430 West Innovation Drive, Apartment 112, Wauwatosa, WI and signed a lease agreement for the property on December 9, 2022. Becker further provided case agents with a copy of SMITH's Wisconsin driver's license, which SMITH provided during the rental application process. Becker further informed case agents that SMITH was assigned parking stall "108" in the underground parking garage.

16. On June 6, 2023, the Honorable Michael J. Hanrahan, Circuit Court Judge for Branch 4 in Milwaukee County, authorized a warrant allowing a certified drug detection canine and its handler to enter onto the curtilage of 10430 West Innovation Drive, Apartment 112, Wauwatosa, WI to conduct a dog sniff.

17. On June 9, 2023, pursuant to a positive alert by the drug detection canine, the Honorable Jean M. Kies, Circuit Court Judge for Branch 45 in Milwaukee County, authorized a warrant to search the premises at 10430 West Innovation Drive, Apartment 112, Wauwatosa, WI.

18. On June 13, 2023, case agents executed the warrant to search 10430 West Innovation Drive, Apartment 112, Wauwatosa, WI (hereinafter, "the premises"). During the execution of the search warrant SMITH along with Desiree D. Washington (DOB: 06-11-90) and a juvenile with the initials D.W were located inside the premises.

19. During a search of the premises, case agents found a black and gray Nike brand shoe box, size 13, inside the left cabinet of the bathroom vanity. The shoe box contained a black

canvas bag that held a tan in color Gucci brand bag. The Gucci bag contained a gray chunk of suspected fentanyl inside a sandwich baggie. The suspected fentanyl was in the shape of a square and appeared to be manufactured in a press. Also inside the shoe box was a second sandwich baggie that contained a tan chunk of suspected fentanyl. The shoebox had a third sandwich baggie that contained an off-white chunk of suspected crack cocaine as well. The suspected controlled substances were later transported to North Central HIDTA where case agents subjected the substances to Nark II field tests no. 2 and no. 33. The suspected fentanyl tested positive for the presence of fentanyl with total weights of 120 grams and 80 grams. The suspected crack cocaine tested positive for the presence of cocaine with a total weight of 40 grams. Case agents inventoried the controlled substances on Milwaukee Police inventory no. 23019110.

20. In a bathroom vanity on the premises, case agents found a black Adidas brand bag that contained a gray in color Magic Bullet brand blender with gray residue inside the blender. The blender was later transported to North Central HIDTA. Case agents subjected a sample of the residue from inside the blender to a Nark II Field test no. 33. The substance tested positive for the presence of fentanyl. Case agents inventoried the Magic Bullet on Milwaukee Police inventory no. 23019092 as item no. 7.

21. Case agents found brown paper bags in the center drawer of the bathroom vanity on the premises. The paper bags contained numerous sandwich baggies with the corners missing. Case agents inventoried the baggies on Milwaukee Police inventory no. 23019114 as item no. 5.

22. Case agents found a white plate in the center drawer of the bathroom vanity on the premises. The white plate contained a tan residue. The plate was later transported to North Central HIDTA. Case agents subjected a sample of the residue to a Nark II field test no. 33. The substance

tested positive for the presence of fentanyl. Case agents inventoried the plate on Milwaukee Police inventory no. 23019092 as item no. 9.

23. Case agents found a black digital gram scale in the center drawer of the bathroom vanity on the premises. The scale was later transported to North Central HIDTA. Case agents inventoried the scale on Milwaukee Police inventory no. 23019092 as item no. 5.

24. Case agents found a black Glock 43X 9mm handgun with serial no. BXCD414. The firearm contained one unspent 9mm cartridge in the chamber and 14 unspent 9mm cartridges in the magazine. Case agents located the Glock in the front pocket of a gray 3XL Nike brand hooded sweatshirt. The sweatshirt was located on the right side of the bed along the headboard in the master bedroom of the premises. The Glock was located with a gold in color necklace with a crown pendant with the word "Huncho" attached to the pendant. The Glock was later transported to North Central HIDTA. Case agents inventoried the item on Milwaukee Police inventory no. 23019100. Case agents later transported the Glock to the Milwaukee Police Department's Forensic Unit for a forensic analysis.

25. Case agents found U.S. currency inside the right front pants pocket of a pair of blue jeans that were recovered from the ground, next to the bed, near the window of the master bedroom of the premises. The blue jeans containing the US currency were size 44. On June 21, 2023, case agents transported the currency to Loomis for an official count. The currency was determined to be \$7,280.00.

26. Case agents found an ETS brand 9mm extended magazine in the premises' master bedroom closet. The magazine contained 15 unspent 9mm cartridges. The magazine was later transported to North Central HIDTA. Case agents inventoried the item on Milwaukee Police inventory no. 23019114.

27. Case agents found a black iPhone with no case and a black Sonim flip style cellular phone on top of a shoe box along southside wall of the premises' master bedroom. The cellular phones later were transported to North Central HIDTA. Case agents inventoried the items on Milwaukee Police Department inventory no. 23019198 as item no. 1 and item no. 2.

28. Case agents as witnessed by Corporal French found a black iPhone with no case and shattered back, and a black iPhone with clear case. The cellular phones were located on the left side of the bed in the premises' master bedroom. The cellular phones were later transported to North Central HIDTA. Case agents inventoried the items on Milwaukee Police Department inventory no. 23019198 as item no. 3 and item no. 4.

29. Case agents found a red iPhone with a Supreme brand case, and a blue iPhone with a clear case and black magnet holder. The cellular phones were located on the right side of the bed in the premises' master bedroom. The cellular phones were later transported to North Central HIDTA. Case agents inventoried the items on Milwaukee Police Department inventory no. 23019198 as item no. 5 and item no. 6.

30. Case agents found a black iPhone with a black case. The cellular phone was on top of the bed in the premises' south bedroom. The cellular phone was later transported to North Central HIDTA. Case agents inventoried the cellular phone on inventory no. 23019198 as item no. 7.

31. Case agents found a blue plate in the bottom right drawer of the kitchen island in the premises. The plate contained an off-white residue. The plate was later transported to North Central HIDTA. Case agents subjected a sample of the residue to a Nark II field test no. 07. The substance tested positive for the presence of cocaine. Case agents inventoried the plate on Milwaukee Police inventory no. 23019092 as item no. 8.

32. Case agents found a Pyrex glass in the cabinet under the sink in the premises. The Pyrex contained an off-white residue. The Pyrex was later transported to North Central HIDTA. Case agents subjected a sample of the residue to a Nark II field test no. 07. The substance tested positive for the presence of cocaine. Case agents inventoried the Pyrex on Milwaukee Police inventory no. 23019092 as item no. 4.

33. Case agents found a black digital gram scale in the second drawer from top of the kitchen island in the premises. The scale was later transported to North Central HIDTA. Case agents inventoried the scale on Milwaukee Police inventory no. 23019092 as item no. 6.

34. Case agents located vehicle keys in the apartment. The keys belonged to a black Chevy Equinox bearing Florida registration 45ASKZ (Vin no. 2GNAXHEVXL6278765) that was parked in the underground garage (stall 108). The vehicle is a rental vehicle with PV Holdings. Nothing of evidentiary value was found in the vehicle.

35. On June 14, 2023, the Honorable Barry Phillips, Court Commissioner for the First Judicial District of Wisconsin, authorized a search warrant to conduct a forensic analysis of the above-referenced cellular phones that were seized during the execution of the search warrant at 10430 West Innovation Drive, Apartment 112, Wauwatosa, WI.

**IDENTIFICATION OF iCloud ACCOUNTS HUNCHOTEZ38@ICLOUD.COM
AND TARSHARTEZ@ICLOUD.COM**

36. Case agents viewed a forensic analysis of the blue iPhone with clear case with black magnet holder that was seized from the master bedroom and later placed on Milwaukee Police inventory no. 23019198 item no. 6. The cellular phone was identified as an iPhone 12 with phone number 414-610-5413 and Apple ID hunchotez38@icloud.com. While viewing text messages sent from this device, case agents learned SMITH was also using a secondary cellular phone with cellular phone number 414-610-2000. Case agents examined a partial forensic analysis of a red iPhone with a Supreme brand case. The red iPhone was located with the aforementioned blue iPhone and later placed on Milwaukee Police inventory no. 23019198 as item no 5. The partial extraction showed the device was a iPhone XR with phone number 414-610-2000 and Apple ID tarshartez@icloud.com.

BACKGROUND CONCERNING APPLE¹

37. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at <https://support.apple.com/kb/PH26502>.

38. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
- c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.
- d. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.
- e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.
- f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.
- g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft

Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

39. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

40. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

41. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

42. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

43. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email

(iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

44. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

45. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

46. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user

attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

47. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

48. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

49. Therefore, Apple’s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple’s services. In my training and

experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

50. Based on the forgoing, I request that the Court issue the proposed search warrant.

51. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with hunchotez38@icloud.com and tarshartez@icloud.com (the “accounts”) that are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the accounts were created, the length of service, the IP address used to register the accounts, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- c. The contents of all emails associated with the accounts from January 1, 2023 to the present, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- d. The contents of all instant messages associated with the accounts from January 1, 2023 to the present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the

accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- f. All activity, connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- g. All records and information regarding locations where the accounts or devices associated with the accounts were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the accounts, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14** **DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, those violations involving Tarsh A. SMITH and others known and unknown, and occurring after January 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The sale of illegal drugs and the laundering of proceeds of drug sales;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to drug trafficking, including records that help reveal their whereabouts.